



Who is required to take this Security Briefing?

IF...	YOU ARE REQUIRED TO...
You are receiving an “L” or “Q” badge from Sandia National Laboratories/New Mexico (SNL/NM) for the first time since being granted a clearance,	<ol style="list-style-type: none">1. Review this booklet.2. Complete the Security Briefing Certification (p. 33).3. Read and sign Standard Form 312, Classified Information Nondisclosure Agreement (pp. 35–36).
You are having clearance reinstated or transferred from another facility,	<ol style="list-style-type: none">1. Review this booklet.2. Complete the Security Briefing Certification (p. 33).3. Read and sign Standard Form 312, Classified Information Nondisclosure Agreement (pp. 35–36).
None of these categories apply to you,	Immediately return this booklet to the Badge Office clerk.


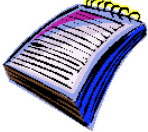


USING THIS BOOKLET

Sandia is continually revising corporate process requirements (CPR) documents to capture the latest requirement changes based on DOE orders, federal and state laws, and Sandia best-management practices. When there is a discrepancy between the CPRs and training, follow the information within the CPRs.

This booklet discusses the important role you play in protecting national security. You have been the subject of a personnel security investigation that was conducted to determine your suitability for access to classified matter. You have been granted access authorization or a security clearance because Sandia may require you to access classified matter or your unescorted access to security areas.

You should become familiar with the contents of this booklet. Your manager will give you specific information about security practices for your individual job and area.


The following symbols will aid in guiding you through this booklet:

	Key Points – the most important points that you need to know about each topic
	Note – specific information of an exceptional or critical nature
	Your Responsibilities – things that you are required to do
	For Your Information – contact information or resources for more details on each topic

CONTENTS

INTRODUCTION	1
RESPONSIBILITIES.....	3
ACCESS AUTHORIZATION	6
DOE REPORTING REQUIREMENTS	9
INSIDE SANDIA.....	13
PROTECTION AND CONTROL OF CLASSIFIED MATTER.....	18
FOREIGN INTERACTIONS	22
SECURITY INFRACTIONS AND VIOLATIONS.....	23
OTHER IMPORTANT INFORMATION	25
REVIEW	31
SECURITY BRIEFING CERTIFICATION.....	33
CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT.....	35

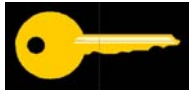
INTRODUCTION

<p>Purpose of This Security Briefing</p>	<ul style="list-style-type: none"> • This briefing fulfills the intent of DOE Order 470.1 (Change 1), <i>Safeguards and Security Program</i> (6/96). This document also serves as: <ul style="list-style-type: none"> ➤ Interim Comprehensive Security Briefing for newly cleared Sandia employees. ➤ Initial/Comprehensive Briefing for newly cleared Sandia contractors and consultants. ➤ Comprehensive Briefing for all reinstated Sandia Members of the Workforce (employees, contractors, and consultants). • This briefing also meets the DOE Manual 471.2-1C, <i>Classified Matter Protection and Control Manual</i>, requirement that training shall be provided before personnel have access to classified matter.
<p>Classified Information Nondisclosure Agreement</p> <p>Your Responsibility</p> 	<ul style="list-style-type: none"> • Standard Form 312 (SF-312), Classified Information Nondisclosure Agreement, is a contractual agreement between the U.S. government and you, a cleared individual, that attests to your loyalty and agreement not to disclose classified information to unauthorized sources. The Agreement also states the consequences if you fail to fulfill your part of the Agreement. • As a condition of access, all persons with Department of Energy (DOE) security clearances are required to read and sign SF-312, Classified Information Nondisclosure Agreement (see last page in this booklet). You shall: <ul style="list-style-type: none"> ➤ Read SF-312. ➤ Sign it. ➤ Return it to the Badge Office clerk.



Security Objectives

Key Points



- As a person with a clearance, you are personally responsible for all **classified matter** and **Unclassified Controlled Information (UCI)** entrusted to you.
- The DOE and SNL/NM have four major security objectives that you should make your own:

1. Protection of Special Nuclear Material (SNM)

As a Class "A" facility, SNL/NM could have SNM, such as uranium and plutonium in various forms, in its inventory at any time. Control and protection of SNM is essential because of its potential damaging use should it fall into unauthorized hands.

2. Protection of Classified Matter

- To ensure that there is no compromise or loss of classified information or material, you shall:
 - Be able to identify unprotected classified matter.
 - Know the appropriate reporting requirements.
- Before allowing access to such matter, you shall establish the requestor's:
 - Identity.
 - Proper clearance access.
 - Official Need to Know.

3. Protection of Sensitive Unclassified Matter

Unclassified Controlled Information (UCI) can aid unauthorized sources to gain valuable help to do harm to our national security. Be alert! Practice denying the collection of sensitive information by unauthorized sources.

4. Protection of Government Property



All property at SNL/NM is owned by DOE and, in essence, the American people. The care of this property is the responsibility of all who work with it. Equipment and resources entrusted to you in your work shall be given due care and accountability.



MANAGERS' RESPONSIBILITIES

Organization Security Briefing	<ul style="list-style-type: none"> • Sandia managers are: <ul style="list-style-type: none"> ➤ Strongly encouraged to instill good security habits in their employees, consultants, and contractors. ➤ Encouraged to promote the proper protection of classified and sensitive unclassified information, government property, and Sandia assets.
---------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

MEMBERS' OF THE WORKFORCE RESPONSIBILITIES

<p>Your Responsibility</p>  <p>For Your Information</p> 	<p>Members of the Workforce (employees, contractors, and consultants) should be sure that:</p> <ul style="list-style-type: none"> • They are made aware of any special rules and/or requirements as they apply to their jobs, buildings, or areas. • They receive additional appropriate training beyond this Security Briefing, if their job responsibilities include the generation, handling, use, storage, reproduction, transmission (including hand carrying), and/or destruction of classified matter. • In any situation they are unsure of, they contact one of the following for clarification: <ul style="list-style-type: none"> ➤ Their responsible manager, Division Security S&S Coordinator, or a Line Training Coordinator. ➤ Security Police Officer. ➤ Corporate Investigators (845-9900). ➤ Security Education (845-9207). ➤ Non-emergency hotline (844-6515).
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



SANDIA EMPLOYEES

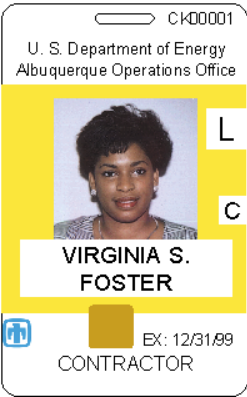
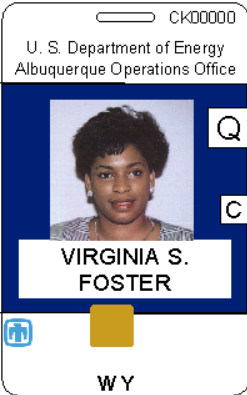

<p>Interim Comprehensive Security Briefing (SEC150I)</p>	<ul style="list-style-type: none"> • This document serves as an Interim Comprehensive Security Briefing to allow Sandia New Mexico employees temporary access to Limited Areas and classified matter, if required. • This training shall be completed before access to classified is allowed. • You will receive notice when due for the in-depth Comprehensive Security Briefing.
<p>Comprehensive Security Briefing (SEC150)</p>	<ul style="list-style-type: none"> • The in-depth Comprehensive Security Briefing: <ul style="list-style-type: none"> ➤ Is mandatory. ➤ Covers subjects in this booklet in detail. ➤ Is approximately 4 hours in duration. • Failure to attend the Comprehensive Security Briefing will result in loss of access to Limited Areas until the briefing has been completed. • Enroll yourself in the Comprehensive Security Briefing through TEDS Everyone at https://tedsprod.sandia.gov/teds/TEDSEveryOne.jsp.
<p>Annual Security Refresher Briefing (SEC100)</p>	<ul style="list-style-type: none"> • All Members of the Workforce (employees, contractors, and consultants) with a DOE clearance shall complete either the hardcopy or online version of the Annual Security Refresher Briefing (SEC100) within 12 months of their last briefing.
<p>Termination Briefing</p>	<ul style="list-style-type: none"> • When your access authorization is terminated, you will receive a Termination Briefing to inform you of your continuing security responsibilities. • The Termination Briefing is held whenever the earliest of the following three events occurs: <ul style="list-style-type: none"> ➤ Last day of your employment. ➤ Last day you possess an access authorization. ➤ Day it becomes known that you no longer require access to classified information or special nuclear materials.




CONTRACTOR or CONSULTANT PERSONNEL

<p>Initial/ Comprehensive Security Briefing (SEC050 & 150)</p>	<ul style="list-style-type: none"> • This document serves as the Initial/Comprehensive Security Briefing for contractors and consultants to inform them of their Safeguards and Security responsibilities. • This briefing is mandatory before: <ul style="list-style-type: none"> ▪ Cleared badge will be issued. ▪ Access to classified is allowed.
<p>Annual Security Briefings (SEC100)</p>	<ul style="list-style-type: none"> • All Sandia National Laboratories, New Mexico, contractors and consultants with a DOE clearance shall complete either the hardcopy or online version of the Annual Security Refresher Briefing (SEC100) within 12 months of their last briefing. • If you are a contractor, annual security briefings are a shared responsibility between your Line manager and your employer. • If you are a consultant, annual security briefings are the responsibility of your Line manager. • Annual security briefings are subject to audit inspection for compliance.
<p>Termination Briefing</p>	<ul style="list-style-type: none"> • When your access authorization is terminated, you will receive a Termination Briefing to inform you of your continuing security responsibilities. • The Termination Briefing is held whenever the earliest of the following three events occurs: <ul style="list-style-type: none"> ➤ Last day of your employment. ➤ Last day you possess an access authorization. ➤ Day it becomes known that you no longer require access to classified information or special nuclear materials.

ACCESS AUTHORIZATION

<p>Clearance Access</p>	<ul style="list-style-type: none"> • Access is the ability and opportunity to obtain knowledge, use, or possession of classified information required by an individual to perform official duties and which is provided on a Need-to-Know basis. • Access is limited to persons with appropriate clearance and a Need to Know in order to accomplish work assignments.
<p>Need to Know</p>	<ul style="list-style-type: none"> • Need to Know is a determination by persons having responsibility for classified information/material and sensitive unclassified information to access such information/material as necessary in the performance of official or contractual duties.
<p>Security Badges</p> <div data-bbox="118 663 363 1056">  </div> <div data-bbox="118 1155 363 1547">  </div> <p>Note</p> 	<ul style="list-style-type: none"> • All Sandia employees, contractors, and consultants are issued DOE Standard Badges, which allow access to Limited Areas (security areas). • Access to classified information/material is granted with the appropriate clearance level and on a Need-to-Know basis. • The most common clearances granted by the DOE at Sandia National Laboratories are the “L” and “Q.” The access authorization permitted by each is listed below. • An “L clearance” (yellow badge) allows access to: <ul style="list-style-type: none"> ➢ Secret Formerly Restricted Data (SFRD) ➢ Secret National Security Information (SNSI) ➢ Confidential Restricted Data (CRD) ➢ Confidential Formerly Restricted Data (CFRD) ➢ Confidential National Security Information (CNSI) ➢ Special Nuclear Material (SNM) Categories II and III ➢ Unescorted access to Limited and Protected Areas • A “Q clearance” (blue badge) allows access to all of the above, plus: <ul style="list-style-type: none"> ➢ Secret Restricted Data (SRD) ➢ Top Secret Restricted Data (TSRD) ➢ Top Secret Formerly Restricted Data (TSFRD) ➢ Top Secret National Security Information (TSNSI) ➢ SNM Category I (only if person has Personnel Security Assurance Program [PSAP] certification, in addition to a Q clearance and Need to Know) • Prior to “Q”-cleared personnel accessing ANY Top Secret (TS) matter, he or she must be authorized for Need to Know. Consult Classification (12225) regarding TS access authorization. • Certain badges authorize the bearer to certain access control areas or access to certain information, such as Weapon Data. <ul style="list-style-type: none"> ➢ The area designation or special information access indicators are shown at the front bottom of the badge. ➢ You shall assure that the individual requesting access to controlled areas or certain information has a Need to Know.

ACCESS AUTHORIZATION (CONT'D.)

<p><i>Your Responsibilities for Your Security Badge</i></p> 	<ul style="list-style-type: none">• It is against the law to counterfeit, alter, or misuse a badge.• If your badge is lost or stolen, report it immediately to the Badge Office (work hours: 284-3626; after hours: 844-3155).• Your badge is the property of DOE and shall be returned to Personnel Security/Badge Office (12223-1) if it is expired, no longer needed, or upon termination.• Do not use the DOE standard badge outside of DOE facilities for other than government purposes.• Sandia employees, consultants, and contractors on extended leave of absence for over 90 days shall return their badge to the Badge Office and call 844-7729.• Upon entering Sandia Limited Areas present your badge for examination by the Security Police Officer or use the automated gates.• You shall:<ul style="list-style-type: none">➤ Wear your badge in plain view, above the waist while in DOE-owned or -leased security areas, including Property Protection Areas.➤ Renew it when contract company or contract number changes.➤ Renew it when your name or physical appearance changes.➤ Renew it if faded or damaged.➤ Remove it when off site—for example, don't wear your badge to restaurants or to obtain an airport parking discount.
<p><i>Reinvestigation</i></p>	<p>Your background is reinvestigated every 5 years following your initial background investigation if you hold a Q clearance and every 10 years if you hold an L clearance.</p>

Suspension/ Termination


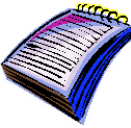

Key Points



- Your security clearance may be suspended or terminated for any of, but not limited to, the following derogatory* reasons:
 - Gross misconduct, failure to protect, or careless handling of classified matter.
 - Disclosure of classified information to a person unauthorized to receive such information.
 - Failure to safeguard special nuclear material.
 - Theft of government property.
 - Association in any act of sabotage, espionage, treason, terrorism, or sedition.
 - Gross violation of or disregard for security or safeguards regulations.
 - Illness or mental condition that significantly impairs an individual's judgment or reliability.
 - Excessive or habitual use of alcohol.
 - Trafficking in, selling, transferring, possessing, or using illicit drugs or controlled substances.
 - Engaging in any unusual conduct that reveals an individual as dishonest, unreliable, or untrustworthy.

*10CFR710.8, *Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material*, lists information that is considered "derogatory." This information casts doubt upon the reliability of personnel to obtain or maintain access authorization to DOE security interests.

DOE REPORTING REQUIREMENTS

<p>General Reporting Requirements</p> <p>Your Responsibility</p> 	<ul style="list-style-type: none"> Executive Order 12968, <i>Access to Classified Information</i>, makes a very serious demand on ALL personnel. It states: “Employees are encouraged and expected to report any information that raises doubts as to whether another employee’s continued eligibility for access to classified information is clearly consistent with the national security.” A common concern is, “What issues raise doubt about a person’s eligibility to be trusted with national security interests?” They are the same issues that were considered when you were being investigated for your clearance. It is your duty and responsibility to: <ul style="list-style-type: none"> ➤ Maintain your access authorization. ➤ Report any doubts about the trustworthiness of those people you work with and around.
<p>Supervisors’ Reporting Requirements</p> <p>Note</p>  <p>For Your Information</p> 	<ul style="list-style-type: none"> In compliance with Sandia Business Rule CPR400.3.7, <i>Security Concerns Reporting Process</i>, and DOE Order 472.1C, <i>Personnel Security Activities</i>, all supervisors aware of the following conditions affecting an applicant’s or employee’s access authorization status, shall provide notification of: <ul style="list-style-type: none"> ➤ An individual’s hospitalization or other treatment for a mental illness or other condition (e.g., substance abuse) that may cause a significant defect in the individual’s judgment or reliability. In addition to notifications detailed below, notify Medical (845-8037) about any of these conditions, on the same schedule. ➤ Information of personnel security interest. Such information must be characterized as reliable and relevant and create a question as to an individual’s access authorization eligibility as exemplified in 10CFR710.8, <i>Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material</i>. Verbal notification shall be provided within 2 working days and written confirmation within the next 10 working days to Personnel Security/Badge Office (844-8742) and Corporate Investigators (845-9900). Notification should not be provided if the individual does not hold, or is not in process of obtaining, a DOE clearance. For more information regarding DOE reporting requirements, consult the following: <ul style="list-style-type: none"> ➤ Corporate Investigators (845-9900). ➤ Personnel Security/Badge Office (844-8742). ➤ CPR400.3.7, <i>Security Concerns Reporting Process</i>.
<p>Maintaining Your Access Authorization</p>	<ul style="list-style-type: none"> Maintaining your security clearance is essential to your job. To maintain your security clearance, you shall follow all reporting requirements, which apply both within and outside of the United States.

DOE REPORTING REQUIREMENTS (CONT'D.)

IF YOU	YOU SHALL REPORT THIS	TO
<ul style="list-style-type: none"> Are arrested, have criminal charges brought against you, or are detained by any law enforcement authority (local, state, OR federal) for violations of the law, regardless if no formal charges have been made, or charges are made but later dismissed. <p>Note: Traffic violations with fines of \$250 or less do not need to be reported.</p>	<ul style="list-style-type: none"> Orally, within 2 working days of occurrence In writing, within the next three working days 	Corporate Investigators (845-9900)
<ul style="list-style-type: none"> File for bankruptcy, regardless of whether it is for personal or business-related reasons. 	<ul style="list-style-type: none"> Orally, within 2 working days of occurrence In writing, within the next three working days 	Corporate Investigators (845-9900)
<ul style="list-style-type: none"> Have your wages garnisheed for ANY reason. <p>Examples: divorce, debts, child support</p>	<ul style="list-style-type: none"> Orally, within 2 working days of occurrence In writing, within the next three working days 	Corporate Investigators (845-9900)
<ul style="list-style-type: none"> Change citizenship or dual citizenship. Name change. 	<ul style="list-style-type: none"> Orally, within 2 working days of occurrence In writing, within the next three working days 	Personnel Security/ Badge Office 844-2007
<ul style="list-style-type: none"> Marry or cohabit with a person who does not currently hold a DOE access authorization (clearance). 	<ul style="list-style-type: none"> In writing (DOE Form 5631.34, Data Report on Spouse), within 45 calendar days of marriage or cohabitation 	Personnel Security/ Badge Office 284-9519
<ul style="list-style-type: none"> Are approached or contacted by ANY individual seeking unauthorized access to classified matter or Special Nuclear Material. 	<ul style="list-style-type: none"> Immediately 	SIMP Pager (540-2382) or Corporate Investigators (845-9900) or Counterintelligence (284-5923)

DOE REPORTING REQUIREMENTS (CONT'D.)

IF YOU	YOU SHALL REPORT THIS	TO
<ul style="list-style-type: none"> Are hospitalized or treated for a mental illness or a mental condition, or for treatment of alcohol or drug abuse. 	<ul style="list-style-type: none"> Immediately 	Medical (845-8037) or Corporate Investigators (845-9900) or Personnel Security/Badge Office (845-9650)
<ul style="list-style-type: none"> Have business-related foreign travel to sensitive countries. Have business-related foreign travel to non-sensitive countries. Have personal foreign travel to sensitive countries. <p>Note: You are not required to report personal foreign travel to non-sensitive countries before your trip; however, keep a personal record of such travel for future clearance investigations.</p>	<ul style="list-style-type: none"> 37 days before trip 28 days before trip 30 days before trip 	Foreign Interactions (845-8488 or 284-4231)
<ul style="list-style-type: none"> Have contact with persons from sensitive countries. Are employed by, represent, or have other business-related association with a foreign or foreign-owned interest, or foreign national. <p>Note: Contact is defined as "a substantive personal or professional relationship."</p>	<ul style="list-style-type: none"> Immediately 	Counterintelligence (284-5923) or Corporate Investigators (845-9900)
<ul style="list-style-type: none"> Are aware of information of personnel security interest. <p>Note: Such information must be characterized as reliable and relevant and create a question as to the individual's access authorization eligibility as documented in 10CFR710.8, <i>Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material</i>.</p>	<ul style="list-style-type: none"> Immediately 	Corporate Investigators (845-9900)

DOE REPORTING REQUIREMENTS (CONT'D.)

<i>Waste, Fraud, & Abuse</i>	<ul style="list-style-type: none"> Incidents of waste, fraud, abuse, and criminal matters shall be reported to SNL Corporate Investigators (845-9900) and other appropriate authorities. The Sandia Ombuds and Ethics Offices (844-1744) are also available.
<i>Theft of Property</i>	<ul style="list-style-type: none"> Any theft of Sandia or U.S. Government property shall be reported immediately to SNL Corporate Investigators (845-9900). All property that is considered stolen, lost, or missing shall be reported regardless of value and regardless of whether it is considered controlled or uncontrolled property.
<i>Wrongdoing</i>	<ul style="list-style-type: none"> In addition to the circumstances listed in the previous table (pp. 10–11), employees, contractors, and consultants shall report Incidents of Wrongdoing to: <ul style="list-style-type: none"> ➤ SNL/NM contacts listed in the previous table. ➤ SNL Corporate Investigators (845-9900). You may also report directly to the Office of the Inspector General any information concerning wrongdoings by DOE employees, contractors, subcontractors, consultants, grantees, or other recipients of DOE financial assistance, or their employees.
<i>Drugs in the Workplace</i>	<ul style="list-style-type: none"> Illegal drugs are prohibited on both Sandia-controlled premises and Kirtland Air Force Base property. Individuals who illegally used or trafficked in a controlled substance may be asked to sign a drug certification form attesting to refraining from using or being involved with illegal drugs while employed in a position requiring a security clearance. The use of illegal drugs is a serious offense and could result in termination of your clearance and, eventually, your employment, as well as arrest. Incidents of illegal drugs in the workplace shall be reported to Corporate Investigators (845-9900). This includes, but is not limited to, trafficking in, selling, transferring, possessing, or using illegal drugs.

Controlled Areas

Key Points







- **Property Protection Areas** – established for the protection of DOE property.
- **Limited Areas** – security areas having boundaries identified by barriers for the protection of classified information
- **Exclusion Areas:**
 - Are another type of security area requiring additional Need-to-Know authorization and usually requiring that permission be obtained before entering.
 - Provide access to classified information.
 - Allow access to both Q- and L-clearance holders. However, some areas of an Exclusion Area may be off-limits to an L-cleared person.
 - Check for posted signs in the areas being accessed.
 - Challenge others in areas where visitors may be present for proper access level.
- **Material Access Areas** – established for the protection of special nuclear material (SNM)

Escorting Uncleared Persons or Visitors



- DOE Q- or L-cleared U.S. citizens can act as escorts.
- Your responsibilities as an escort **anywhere on Sandia-controlled premises** are:
 - **Do not** exceed eight uncleared personnel per escort.
 - Brief uncleared personnel about evacuation procedures and how to report emergencies.
 - Ensure that uncleared personnel are badged.
 - Ensure that uncleared personnel follow rules and signs.
 - If escort responsibility is transferred, ensure that new escorts are aware of their responsibilities.
 - Ensure that uncleared personnel surrender their badges per instructions on their orange card (SA 2730-CB).
- **Uncleared U.S. citizens** with appropriate DOE-approved badges may:
 - **NOT** be escorted into Material Access Areas (MAAs), Exclusion Areas, certain vaults, and classified computer centers.
 - Be escorted into Limited Areas for authorized and essential business activities.
 - Enter Property Protection Areas (PPAs) without an escort.
- Within **Limited or more restricted areas**, only a U.S. citizen, Sandia employee, contractor, or consultant, with a Q or L clearance and DOE-approved badge may escort.
- Escort responsibilities are:
 - Remain with the uncleared personnel (UP) at all times.
 - Ensure that uncleared personnel **do not** gain access to classified.
 - Inform UP of prohibited items.
 - Allow access by uncleared personnel through automated gates, using your badge and personal identification number (PIN).
 - If visit ends later than 6 p.m., notify SNL/NM Security (844-4657 or 844-4658).
- **Uncleared-visitor badges** have a diagonally striped gray background.
- **Visitors** may have unescorted or escorted access to Limited Areas, depending on their access authorization and their Need to Know.

<p>Search Policy</p> <p>Key Points</p> 	<ul style="list-style-type: none"> • Upon entering or leaving Sandia-controlled premises, all personnel are subject to search of their persons, hand-carried items, and vehicles to ensure that: <ul style="list-style-type: none"> ➤ No contraband is being introduced. ➤ No government property or classified information/material is being removed without proper authorization. • A Security Police Officer may ask you to submit all containers for examination. Containers include packages, boxes, briefcases, handbags, etc.
<p>Prohibited Items</p> <p>Key Points</p> 	<ul style="list-style-type: none"> • Items prohibited on Sandia-controlled premises without prior authorization include: <ul style="list-style-type: none"> ➤ Firearms. ➤ Explosives, pyrotechnics, propellants. ➤ Illegal drugs and paraphernalia, intoxicants. ➤ Other items prohibited by law. • Personally owned items prohibited within Limited and more restricted areas without prior authorization include: <ul style="list-style-type: none"> ➤ Radio frequency-transmitting equipment. ➤ Recording equipment (audio, video, data). ➤ Computers, peripherals, associated media. ➤ Cell phones. ➤ Portable electronics (including hand-held computing devices). • A sign regarding prohibited and controlled items is posted at all access gates. • For additional requirements and information, see CPR400.3.10, <i>Prohibited and Controlled Items</i>, and CPR400.3.16, <i>Cellular Phones</i>.
<p>Personal Vehicle Access</p>	<ul style="list-style-type: none"> • Employee, contractor, and consultant personal vehicles are not permitted in Limited Areas. • Exceptions, such as for health reasons, shall first be approved by Medical (up to 90 days) or Personnel Security/Badge Office (over 90 days). • If you have a state-issued handicap placard and require parking inside a Limited Area, call 284-3958. • Private and contractor company vehicles are always subject to search upon entering and exiting Limited Areas.

<p>After Hours</p> <p>Your Responsibility</p>  <p>For Your Information</p> 	<ul style="list-style-type: none"> • After normal working hours most buildings at SNL are locked and alarmed. • Many buildings are controlled by an access-control system; presence of the system is indicated by badge-swipe equipment and/or a keypad for entering a personal identification number (PIN). Some buildings are controlled 24 hours a day, and some are controlled only after working hours. • If you need access to a corporate access-controlled building, contact the building owner and ask to be added to the access list. • Ask the building owner for proper exiting procedures for times when you must work after hours. Some access-controlled buildings are configured in such a way that you do not have to call Security first before leaving the building after hours. Some buildings, however, do require that you notify Security first; the numbers to call are 844-4657 or 845-3114. • If you find yourself within a building or an area where there appears to be no way out, you should look for a turnstile or locate a phone and call for assistance. <ul style="list-style-type: none"> ➤ The Key Service number is North (844-4657) or South (845-3114). (South encompasses Tech Areas III and V.) ➤ The emergency number is 911. ➤ Most phones have these numbers posted. • Do not exit the building or area by any means other than the conventional way.
<p>Vouching</p>	<ul style="list-style-type: none"> • Security is frequently asked questions regarding use of badges to swipe in other persons. The following questions are asked most often: <ul style="list-style-type: none"> ➤ What options do I have when asked to vouch someone into a Limited Area? ➤ If the person has an apparently valid Q or L badge, should you let him or her enter the Limited Area? ➤ When should you suggest that the person go to a manned gate or to the Badge Office? • There may be various reasons why another individual's badge is not allowing him or her access through an automated access point. The following background sets the stage for the answers to the questions above: <ul style="list-style-type: none"> ➤ Badge holders have become so proficient at swiping badges that 97% are granted access on the first swipe. ➤ Although there are occasional equipment failures, the general rule is that people who have not gained access after multiple swipes should go to the Badge Office (12223-1) (Building 800).

Key Points



- **Vouching** is a term used to describe when one person allows another access.
- When you vouch for another person, it is assumed that you accept the responsibility and consequences of allowing that person into the area.
- At SNL/NM, there have been some experiences of people misusing the vouching privilege. Two examples follow:
 - A person whose badge would not work went to several gates and asked people to swipe him in. Security had deactivated his badge but had not been able to retrieve it. His badge still appeared valid.
 - One person claimed that his badge was left in the Limited Area and asked people to swipe him in so that he could retrieve it.
- Sandia-issued badges have a blue thunderbird in the lower part of the badge.
- DOE badges from other sites do **not** work in Sandia's system unless they have been enrolled in the Badge Office (12223-1). Once the Badge Office enrolls them, badges from other DOE sites will work in Sandia's system.
- It is appropriate for you to grant access to another person if you feel that you can vouch for his or her entry into a Limited Area. Before you grant access, ask yourself:
 - How much risk do I want to accept?
 - Is the individual's badge a DOE-approved badge?
 - Does the badge look altered in any way?
 - How well do I know this person?
- If you feel uncomfortable with your answers to any of these questions, send the person to the Badge Office (Building 800) (844-8742) or to a manned gate.
- See CPR400.3.11, *Access Controls*, for additional access requirements and information.


Your Responsibility




For Your Information



PROTECTION AND CONTROL OF CLASSIFIED MATTER

<p>Why We Classify</p>	<ul style="list-style-type: none"> • All classified information/material is protected according to federal statutes and Presidential Executive Orders. DOE is responsible, under the Atomic Energy Act of 1954, as amended, for classifying information and material relating to atomic energy and its use in weapons and under Executive Orders for other aspects of national security. The Atomic Energy Act of 1954 and Executive Order 12958 govern classification policy. • Classifying establishes protective barriers that ensure that classified information and material do not fall into unauthorized hands. Through the process of classification, we protect important information from adversaries, yet allow the same information to be used by scientists, statesmen, military planners, and others with applicable access authorization and the Need to Know. • A derivative classifier (DC) determines the appropriate classification level, category, and any required caveats. The classification process is particularly crucial to DOE because its responsibilities include the development and production of nuclear weapons.
<p>Categories of Classified Matter</p> <p>Key Points</p> 	<ul style="list-style-type: none"> • Information and material are classified according to two areas: <ul style="list-style-type: none"> ➤ Categories specify the types of information or material. ➤ Levels indicate the degree of damage that could incur to national security should that information or material be compromised. • There are three categories of classified matter: <ol style="list-style-type: none"> 1. Restricted Data (RD) All data concerning design, manufacture, or utilization of atomic weapons; the production of special nuclear material (SNM); or the use of SNM in the production of energy, but shall not include data declassified or removed from the RD category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended. Examples of technologies categorized as RD are nuclear assembly design, firing and detonating systems, initiators, nuclear safing mechanisms, inertial confinement fusion, and isotope separation. RD is, generally, the most restrictive of the three classification categories. 2. Formerly Restricted Data (FRD) Classified information jointly determined by the DOE or its predecessors and Department of Defense (DoD) to be related primarily to the military utilization of atomic weapons, and removed by the DOE from the RD category pursuant to Section 142(d) of the Atomic Energy Act of 1954, as amended, and safeguarded as National Security Information, subject to the restrictions on transmission to other countries and regional defense organizations that apply to RD. Examples of technologies of the FRD category are fuzing designs, weapons yields, weapon location information, command and control systems, and certain other information the military needs to carry out its nuclear weapons responsibilities. 3. National Security Information (NSI) Information that has been determined, pursuant to Executive Order 12958 or any predecessor order, to require protection against unauthorized disclosure and that is so designated. The levels Top Secret, Secret, and Confidential are used to designate such information. Examples are information related to Safeguards and Security, nuclear reactor site security, and weapon carriers (e.g., missile and aircraft units).

PROTECTION AND CONTROL OF CLASSIFIED MATTER (CONT'D.)

<p>Levels of Classified Information and Matter</p> <p>Key Points</p> 	<ul style="list-style-type: none"> The classification level indicates how sensitive the information or material is. There are three levels of classified information or matter: <ol style="list-style-type: none"> 1. Top Secret (TS) Unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security in a way that the appropriate official can identify or describe. 2. Secret (S) Unauthorized disclosure could reasonably be expected to cause serious damage to national security in a way that the appropriate official can identify or describe. 3. Confidential (C) Unauthorized disclosure could reasonably be expected to cause undue risk to the common defense and security in the case of RD/FRD, or damage the national security in the case of NSI, in a way that the appropriate official can identify or describe. Information and materials vary in their importance to national security. The more sensitive the level, the greater the risk of damage to national security if disclosed to unauthorized sources.
<p>Multiple Classification</p>	<ul style="list-style-type: none"> Only one classification for an entire classified work can exist, and that classification shall be the highest classification category and level of any part of the work. Multiple classifications cannot exist for complete documents or materials, although the “part” may have different classifications. RD and FRD cannot have portion markings.
<p>Determining Proper Classification</p>	<ul style="list-style-type: none"> DCs, many of whom are managers, are the only persons authorized to make classification determinations. You may seek the assistance of classification analysts, who also are DCs, in Classification and Information Security (12225), when necessary.

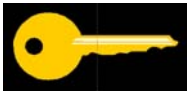
PROTECTION AND CONTROL OF CLASSIFIED MATTER (CONT'D.)

Classified Matter Protection & Control (CMPC)

Your Responsibility



Key Points



- Not every one at SNL/NM works with, or comes in contact with, classified matter. However, the following key points are the MINIMUM areas with which you should be familiar.

If your work responsibilities involve handling classified matter, you shall receive additional training beyond this Security Briefing.

CONTROLLING CLASSIFIED MATTER

- Control classified matter against unauthorized access at all times.
- Report lost or unaccounted for classified matter immediately to the Security Incident Management Program (SIMP) (24-hour pager: 540-2382).
- Manage classified matter in established control stations assigned to an appropriate classified matter custodian.


ACCESSING CLASSIFIED MATTER

- Access to classified matter is the responsibility of the handler.
- Ensure that personnel have the proper clearance level and Need to Know before permitting them to have access to classified matter.

CREATING CLASSIFIED MATTER

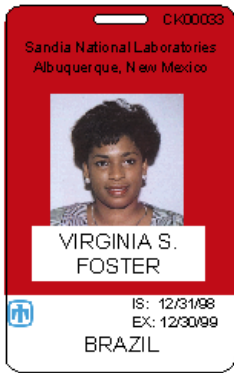
- Classified matter shall be marked appropriately.
- Originators shall have proper classification review performed and apply proper marking requirements for drafts and final documents.
- Classified custodians assist in reviewing markings and marking classified matter.
- Appropriate cover sheets shall be used.

PROTECTION AND CONTROL OF CLASSIFIED MATTER (CONT'D.)

<p>USING CLASSIFIED MATTER</p> <p>STORING CLASSIFIED MATTER</p> <p>MOVING CLASSIFIED MATTER</p> <p>DESTROYING CLASSIFIED INFORMATION</p>	<ul style="list-style-type: none"> • Whenever classified information is in use, it shall be: <ul style="list-style-type: none"> ➤ Within line of sight. ➤ Under personal attendance. • Control may be relinquished only to those who have the appropriate clearance and Need to Know. • Reproduce classified in coordination with the classified matter custodian. • A minimum number of copies should be prepared consistent with operational necessity. • Copier shall be approved to copy classified. • Marking of classified matter is the responsibility of the originator. • Protect classified matter by securing it in an approved repository when not in use. • Approved repositories are GSA-approved safes, approved vaults, and vault-type rooms (VTRs). • Mail, ship, or hand carry classified matter only to authorized recipients and those with a Need to Know. • Use SNL mail and shipping services only to mail and ship classified matter. <ul style="list-style-type: none"> ➤ Internal recipients shall have an approved control station. ➤ External recipients shall have a Sandia-approved Mail Channel. • If classified information has access control markings, the originator shall ensure that the intended recipient has the appropriate access authorization for that access (e.g., Weapon Data, NOFORN). • Handcarry classified matter as a last resort and only if you have: <ul style="list-style-type: none"> ➤ Taken the Annual Handcarry Briefing (SF 2902-AHB). ➤ Written authorization from your manager. • Double wrap documents or use SNL-authorized double handcarry bags when transporting classified outside of a Limited Area. • Receipts for classified matter shall be created and signed, as required in CPR400.3.12, <i>Management of Classified Matter</i>. • Destroy classified matter in accordance with the Sandia Records Retention and Disposition Schedule. • Coordinate destruction with the appropriate classified matter custodian. • Use destruction methods that are approved to ensure classified matter is physically altered, demolished, or reduced to a useless form in such a way that no classified information can be obtained from it.
<p>For Your Information</p> 	<ul style="list-style-type: none"> • Refer any questions regarding classified information or matter to the Classified Matter Protection & Control Program in Information Security (12224). • Direct questions about Mail/Shipping Channels to the Mail Channel Coordinator (844-8008).

FOREIGN INTERACTIONS

Foreign Visitors



- Uncleared Foreign National Site-Specific badges have a red background.
- Sandia employees hosting uncleared foreign nationals at onsite or offsite facilities (e.g., Coronado Club, Hilton) to discuss Sandia and/or DOE business, regardless of whether the event is in Albuquerque or elsewhere in the United States, are required to submit a Foreign National Request (FNR)/Security Plan (SF 7643-FN), to the Foreign Interactions Office (12224-1) for approval, **prior to the visit and in accordance with applicable time requirements.**
- **Attention: Do not** vouch red badges for entry into a Limited Area unless you are the approved host/escort on the FNR/Security Plan.
- Individuals with red badges are required to have an approved FNR/Security plan that documents **all** of the following:
 - Individuals who are approved to host/escort the foreign national.
 - Approved buildings and rooms.
 - Approved visit dates.
- Forms and requirements on interacting with foreign nationals can be found on Sandia's Internal Web.

Foreign Travel


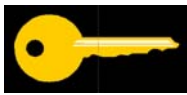
Key Points



- Be aware that there are many restrictions regarding the equipment you may take on foreign travel and that a long lead time is necessary when planning trips.
- All official foreign travel shall be approved through the Foreign Interactions Office (12224-1) prior to departure.
- All personal foreign travel to sensitive countries shall be reported to the Foreign Interactions Office (12224-1) at least 30 days prior to departure.
- For details and requirements consult the Foreign Travel Security Analysts (845-8488 or 284-4231).
- Anyone (e.g., employee, contractor, consultant, retiree) who currently holds a DOE security clearance or has held such a clearance within the last 5 years shall report all foreign travel to sensitive countries for **5 years** following termination or retirement from Sandia.
- As of the date of this document, the following are **sensitive foreign countries** (asterisk [*] denotes terrorist countries):

Algeria	India	Libya*	Syria*
Armenia	Iran*	Moldova	Taiwan
Azerbaijan	Iraq*	North Korea*	Tajikistan
Belarus	Israel	Pakistan	Turkmenistan
China	Kazakhstan	Russia	Ukraine
Cuba*	Kyrgyzstan	Sudan*	Uzbekistan
Georgia			
- Caution should be exercised in dealing with citizens of any country to ensure that sensitive information, although unclassified in nature, is not inadvertently disclosed. This would include nuclear and other U.S. technology and economic information.

SECURITY INFRACTIONS AND VIOLATIONS

<p>Counter-intelligence</p> <p>For Your Information</p> 	<ul style="list-style-type: none"> • Sandia's Office of Counterintelligence (OCI) identifies and counters foreign intelligence targeting Sandia personnel, information, and technologies. • Members of the Workforce (employees, contractors, and consultants) should notify OCI about ANY strange, curious, or suspicious occurrences, whether they happen here or abroad. <p>For further information about:</p> <ul style="list-style-type: none"> • Foreign national policies and procedures, consult Foreign Interactions Office (12224-1). • Foreign Travel, consult Foreign Travel Security Analysts (12224-1) (845-8488 or 284-4231). • Counterintelligence, consult Office of Counterintelligence (5001).
<p>Infractions</p> <p>Key Points</p> 	<ul style="list-style-type: none"> • Security infractions are issued in response to a breach of DOE or Sandia security rules either because of carelessness or ignorance. <ul style="list-style-type: none"> ➤ Sandia Security representative from the Security Incident Management Program (3131) conducts a fact-finding inquiry. ➤ Infractions are reported to DOE. ➤ Corrective action is always required after the occurrence of an infraction is issued. • Here are a few examples of Security Incidents that could result in an infraction being issued: <ul style="list-style-type: none"> ➤ Leaving a classified repository unattended or unsecured. ➤ Failing to account for classified matter. ➤ Failing to maintain prescribed records for accountable classified matter. ➤ Removing classified matter from a Security Area without proper authority. ➤ Discussing classified information over unsecured telephones. ➤ Not obtaining classification guidance, causing compromise of classified information. ➤ Failing to properly mark classified matter as determined by classification authority. ➤ Changing classification of documents without proper authorization. ➤ Failing to properly safeguard repository combinations. ➤ Improperly destroying classified information. ➤ Improperly transmitting classified matter (hand carries, mail, fax, phone, or e-mail). ➤ Improperly escorting uncleared visitors in Security Areas. ➤ Introducing prohibited items (such as personal computers and cellular phones) into Security Areas.

Infraction Penalty System

Key Points



For Your Information



- **Security Infractions**

- Sandia employees and consultants:
 - Consequences of a Security Infraction range from coaching and counseling, to suspension or termination, in accordance with Sandia's disciplinary guidelines.
 - A supervisor is responsible for applying disciplinary action for Security Infractions.
 - Corrective action is required and shall be reported in writing to the Security Incident Management Program (3131) to be forwarded to DOE.
- Contractors – Discipline is the responsibility of the subcontractor's management.

- **Violations**

- Sandia management is responsible for taking corrective action and reporting in writing to the SNL Corporate Investigators (12100).
- Violations are a criminal breach of federal law and can be acts of deliberate intent to harm national interests.
- Severe criminal penalties, including termination and imprisonment or both, may be imposed for security violations.

If you have questions or need details concerning security infractions, consult the Security Incident Management Program (3131) (845-8583).

If you have questions or need details concerning security violations, consult the SNL Corporate Investigators (12100) (845-9900).

OTHER IMPORTANT INFORMATION

Operations Security (OPSEC)

- **National Security Decision Directive 298, OPSEC**

In 1988, President Ronald Reagan issued National Security Decision Directive 298 (NSDD 298), which established a National Operations Security Program. The directive details how each executive department and agency assigned or supporting national security missions with classified or sensitive activities shall establish a formal OPSEC program.

The directive describes OPSEC as a systematic and proven process by which the U.S. Government and its supporting contractors can ***deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities.***

DOE complied with the directive by creating DOE Order 471.2A, *Information Security Program*. DOE Order 471.2A, Chapter 2, "Operations Security Program," details the OPSEC program.

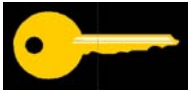
- **SNL/NM's OPSEC Program**

The **purpose** of Sandia's OPSEC Program is to develop OPSEC techniques and measures to enhance the safeguarding of classified, sensitive unclassified and proprietary information against unauthorized disclosure or inadvertent release to unauthorized personnel. OPSEC, then, is a set of procedures and methodologies that provides a way for program, project, or facility managers to implement cost-effective measures to protect programs and staff from exploitation by adversaries.

- The **key to effective OPSEC** is to determine both what critical information most needs to be protected and how a potential adversary would most likely attempt to exploit weaknesses to obtain that information.
- The OPSEC Program applies to all classified and sensitive activities conducted at SNL/NM.
- **OPSEC's five-step process is to:**
 1. Identify critical information.
 2. Analyze threats.
 3. Analyze vulnerabilities.
 4. Assess risk.
 5. Apply appropriate countermeasures.

OTHER IMPORTANT INFORMATION (CONT'D.)

Key Points



- The five primary categories in which adversaries collect intelligence are:
 - Human Intelligence (HUMINT) – Derived from or collected by human resources.
 - Open Source Intelligence (OSINT) – Information gathered from public sources, such as the internet, environmental impact statements, TV, and radio.
 - Imagery Intelligence (IMINT) – Imaging from satellites to hand-held cameras.
 - Signals Intelligence (SIGINT) – Signals from communications: voice, video, Morse code, facsimile.
 - Measurements and Signature Intelligence (MASINT) – Quantitative and qualitative analysis of data from technical sensors.
- Adversaries thrive on collecting many pieces of information they can pull together—like combining puzzle pieces—to discover information about critical programs. A strong OPSEC foundation is built on:
 - Taking steps to protect your information daily, which will lead to a life-long habit of practicing good OPSEC.
 - Team effort—an OPSEC program is only as strong as its weakest player.
 - The individual who is informed and aware is the most important part of an OPSEC program.
- **Practice OPSEC** when:
 - Using non-secure telephones and fax machines.
 - Working with computers and e-mail communications.
 - Involved in casual conversations at work or off site after hours.
 - Disposing of trash or recycled paper.
 - Conducting routine business activities.
- **OPSEC Reviews:**
 - Will be performed in each organization that handles sensitive information at a frequency designated by DOE Order 471.2A, *Information Security Program*.
 - Are conducted to determine the level of OPSEC support required by a program or facility.
 - Are *fact finding*, not fault finding, and will provide organizations with the details needed to make informed decisions regarding future OPSEC support.

OTHER IMPORTANT INFORMATION (CONT'D.)

Technical Surveillance Counter-measures (TSCM)

Your Responsibility



- The purpose of the TSCM Program is to deter unauthorized clandestine technical intelligence collection and to ensure that any overt surveillance is undertaken only under certain circumstances, subject to the requirements of CPR400.3.1, *Technical Surveillance – Audio and Video Recording*.
- TSCM personnel conduct activities under the auspices of the TSCM Program for the purpose of identifying exploitable security weaknesses and enhancing technical and physical security.
- The TSCM Program uses techniques and measures to detect and nullify a wide variety of technologies that are used to clandestinely obtain unauthorized access to classified national security information, restricted data, and/or sensitive but unclassified information.
- Your responsibilities under the TSCM Program include reporting suspected technical penetrations or clandestine audio and video equipment immediately and taking the following steps:
 - Stop all classified or sensitive discussions.
 - Secure the area so that no one can remove or modify the device.
 - Contact the TSCM Team from a location outside the area.
- For additional information about contacting the TSCM Team, see the TSCM section of CPR400.3.1, *Technical Surveillance – Audio and Video Recording*.
- The TSCM Team is linked from the Electronic Security (12222) home page.

OTHER IMPORTANT INFORMATION (CONT'D.)

Technical Surveillance Equipment (TSE) & Potential TSE (PTSE)

Technical Surveillance Equipment

- An example of what is considered TSE is equipment that is commonly developed for law enforcement actions, e.g., wireless microphones worn on the body, or miniature cameras inserted in clocks. This equipment allows law enforcement personnel to survey criminal activity.
- Some SNL operations use equipment that was purchased for legitimate business needs but that is capable of being used as TSE in its "as purchased" state. Some examples of this type of equipment would be wireless microphones, wireless cameras, and radio frequency transmitters. Sandia has developed requirements regarding the acquisition, possession, and use of TSE to ensure its proper use. Consult CPR400.3.1, *Technical Surveillance – Audio and Video Recording*, for those requirements.
- TSE may be allowed in OVERT surveillance of business operations such as a part of an SNL project (e.g., an observation tool to record an ongoing laboratory experiment/project), or for health safety or ES&H concerns. The owners of such devices are required by CPR400.3.1, *Technical Surveillance – Audio and Video Recording*, to ensure that a plan is developed for the protection and control of such devices.
- Areas with active surveillance equipment (even if the equipment is NOT portable) shall have signs posted to inform personnel of its presence.

Potential Technical Surveillance Equipment

- Current concerns affecting most Sandians are the types of equipment known as PTSE., which includes some commercial equipment that, although not designed to be surveillance equipment, could be used as such if employed illegally.
- In general, PTSE that shall be registered with TSCM, according to CPR400.3.1, *Technical Surveillance – Audio and Video Recording*, consists of portable audio and visual data recording devices. The following list of PTSE is **not** comprehensive and is included here for GUIDANCE ONLY.

Digital Cameras	35mm Cameras
Video Cameras	Microphones
Scanning Pens or other portable scanning devices	Palm Pilot-type digital camera or audio recording attachments
MP3 players	Dictaphones and digital voice recorders
- Equipment maintained or installed in a Sandia-owned or -controlled Property Protection Area (PPA) is exempt from registration requirements. Local Line management may institute their own control and inventory methods for equipment kept in a PPA. Equipment that is stored, maintained, or installed in a Limited or more restricted area shall be controlled according to the CPR.
- For information about exemptions, consult CPR400.3.1, *Technical Surveillance – Audio and Video Recording*. If the equipment is not covered by another CPR and is not exempt, register PTSE by using SF2925-TSE, Registration of Potential Technical Surveillance Equipment (Potential TSE), or a specially developed plan.

OTHER IMPORTANT INFORMATION (CONT'D.)

CELLULAR TELEPHONES

Key Points






- **Non-government-purchased cellular phones** (a.k.a. privately owned) are prohibited inside SNL/NM Limited and Protected Areas but are allowed in some Property Protection Areas.
- Non-government-purchased cellular phones may be permitted in Limited Areas under special circumstances (medical exemptions, etc.). Submit SF 7643-POC, Cellular Phone Approval – Non-Government Phones at SNL, for approval.
- Non-Sandia, government-purchased cellular phones shall be identified as such before they are permitted into Limited Areas.
- **Sandia-purchased cellular phones** must have prior authorization to be stored and used within SNL/NM Limited and more restricted areas. Those phones are limited to certain makes and models that have been approved for use in those areas. The phones **shall**:
 - Be registered by submitting SF 7643-PUR, Sandia-Purchased Cellular Phone Security Registration, to Electronic Security (12222).
 - Be authorized for use by Electronic Security (12222). Those phones must have a critical safety or security mission use. Request authorization by filing SF 7643-USE, Cellular Phone Critical Use, with Electronic Security. If approved, a Critical Use Authorization card will be issued.
 - Have a blue Sandia property sticker affixed.
 - Be turned “OFF.” Cellular phone may be used only as necessary for safety and security reasons in support of critical operations, or to report an emergency (844-0911).
- A limited number of Sandia-purchased cellular phones are authorized for use in a Limited Areas. These shall be registered using SF 7643-USE, Cellular Phone Critical Use.
- Cellular phone users shall comply with Line and site-specific cellular phone rules and restrictions.
- Call 845-0699 with questions concerning cellular phones.
- For additional information, see CPR400.3.16, *Cellular Phones*.
- While in Limited Areas:

Note



- Any authorized non-government-purchased cellular phone shall be turned off and locked in a personal or contractor company vehicle authorized to park in the SNL/NM Limited Area.
- Any Sandia- or government-purchased phone shall be turned off (preferably with the batteries removed) unless properly registered, using SF 7643-USE, Cellular Phone Critical Use.

OTHER IMPORTANT INFORMATION (CONT'D.)

<p>PERSONAL DATA ASSISTANTS (PDAs) AND PAGERS</p> <p>Key Points</p> 	<ul style="list-style-type: none"> • Personally owned small electronic items (e.g., Palm Pilots, data organizers, pocket PCs) are not permitted in Limited Areas. • Sandia- or government-purchased small electronic items are permitted but shall be identified as such. Some security areas require technical surveillance countermeasure inspection of Palm Pilots and other PDAs before they are permitted in the areas. • Palm Pilots and other PDAs with recording (e.g., modem, microphone, camera) or radio frequency (RF) transmitting capability are not permitted in Limited Areas, regardless of ownership. • Pagers with transmitting capabilities are not permitted in Limited Areas and some Property Protection Areas. • Call 844-4948 with questions concerning small electronic items.
<p>Classified Discussions</p> <p>MEDIA RELATIONS</p> <p>Computer Security</p> <p>Key Points</p>  <p>For Your Information</p> 	<ul style="list-style-type: none"> • Do not discuss classified information outside Limited Areas. • Never discuss classified or unclassified sensitive information over a non-secure telephone or near an in-use telephone. • If there will be a classified discussion in a Limited Area, power off Sandia-approved cellular telephones and remove the batteries. • Public media reports of classified work at SNL/NM should not be affirmed, denied, or commented upon. • You are responsible to protect the computer you use in the course of your work, and comply with all public laws and DOE/Sandia regulations. • DOE and Sandia have regulations regarding information generated on computers, particularly sensitive unclassified and classified information. • Public laws also require that you protect information generated on computers from waste, fraud, and abuse. Other prohibitions are: <ul style="list-style-type: none"> ➤ Processing Unclassified Controlled Information (UCI) and classified data on unauthorized computers. ➤ Violating copyright and licensing restrictions. ➤ Playing games and using computers for personal applications. ➤ Destroying or modifying hardware, software, or data without authorization. • For more information or if questions arise, consult your Computer Security Representative (CSR). • Contact the following departments, for more information about: <ul style="list-style-type: none"> ➤ Cell phone policies: Electronic Security (12222). ➤ Public media reports: Media Relations (12640). ➤ Computer security: Computer Security and Passwords.
<p>Electronic Security (12222)</p>	<ul style="list-style-type: none"> • Electronic Security installs, designs, and maintains the building alarms, vault and vault-type room (VTR) alarms, and badge readers at all entry-controlled access points, as well as on vaults, VTRs, and other restricted-access areas. • Contacts: See the Electronic Security home page.



Report all:

- Cases of waste, fraud, and abuse.
- Thefts of government property immediately.
- Personal foreign travel to sensitive countries.
- Foreign travel for DOE or other government agencies.
- Close and continuing contact with persons from sensitive countries.
- Arrests and all traffic fines of \$250 or more in writing within 5 working days.
- Illegal or unauthorized access to sensitive matter or special nuclear material (SNM).

Security depends on YOU! Remember—

- If you are a newly cleared Sandia employee (including students), you are required to attend the next in-depth Comprehensive Security Briefing. Registration is available only through the Training, Education, and Development System (TEDS).
- Be aware that your access to classified matter is based on your clearance level and Need to Know.
- Protect classified matter to the best of your ability.
- Coordinate handling of classified matter with an appropriate classified matter custodian.
- Wear your badge in plain view and above the waist at all times while on Sandia property.
- Remove your badge when **not** on Sandia property (e.g., when in restaurants, grocery stores, public areas).
- **Do not** use government property for personal use.
- Illegal drugs should **not** be used and are prohibited at all Sandia properties.
- Personal vehicles may **not** be brought into any SNL/NM Limited Areas unless approved.
- All visits by Foreign Nationals on or off Sandia-controlled properties require approval from Sandia's Foreign Interactions Office (12224-1) and DOE.
- Report marriage or cohabitation in writing within 45 days and name changes on the following schedule: orally, within 2 days; in writing, within the next 3 days.

For Your Information



Further safeguards and security information can be found on the Sandia restricted network at http://www-irn.sandia.gov/security/safeguards_man/home.html.

This page intentionally left blank.

SECURITY BRIEFING CERTIFICATION

- Review and sign (where appropriate) the respective documents listed below.
- Return them to the Badge Office Clerk.

IF YOU ARE...	AFTER REVIEWING THIS BOOKLET, YOU ARE REQUIRED TO...
You are receiving an “L” or “Q” badge from Sandia National Laboratories/ New Mexico (SNL/NM) for the first time since being granted a clearance,	<ul style="list-style-type: none">• Complete the Security Briefing Certification (below).• Read and sign Standard Form 312, Classified Information Nondisclosure Agreement (pp. 35–36).
Having clearance reinstated or transferred from another facility,	<ul style="list-style-type: none">• Complete the Security Briefing Certification (below).• Read and sign Standard Form 312, Classified Information Nondisclosure Agreement (pp. 35–36).



Sandia National Laboratories

New Mexico

Security Briefing Certification

Please Print

CIRCLE ONE: → **SANDIA EMPLOYEE** **CONTRACTOR** **CONSULTANT** **STUDENT**

Name: _____

Signature: _____ Date: _____

Social Security #: _____ Assigned to Sandia Organization: _____

Is your clearance being **reinstated** or **transferred** from another facility? ☐ YES ☐ NO

For Badge Office Use Only

SNL/NM Official: _____ Date: _____

This page intentionally left blank.

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN

AND THE UNITED STATES

(Name of Individual – Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 12958, or under any other Executive Order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952, and 1924, Title 18, *the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Sections 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b) (8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, 952, and 1924 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER (See notice below.)
ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) (Type or Print)		

WITNESS		ACCEPTANCE	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS (Type or Print)		NAME AND ADDRESS (Type or Print)	

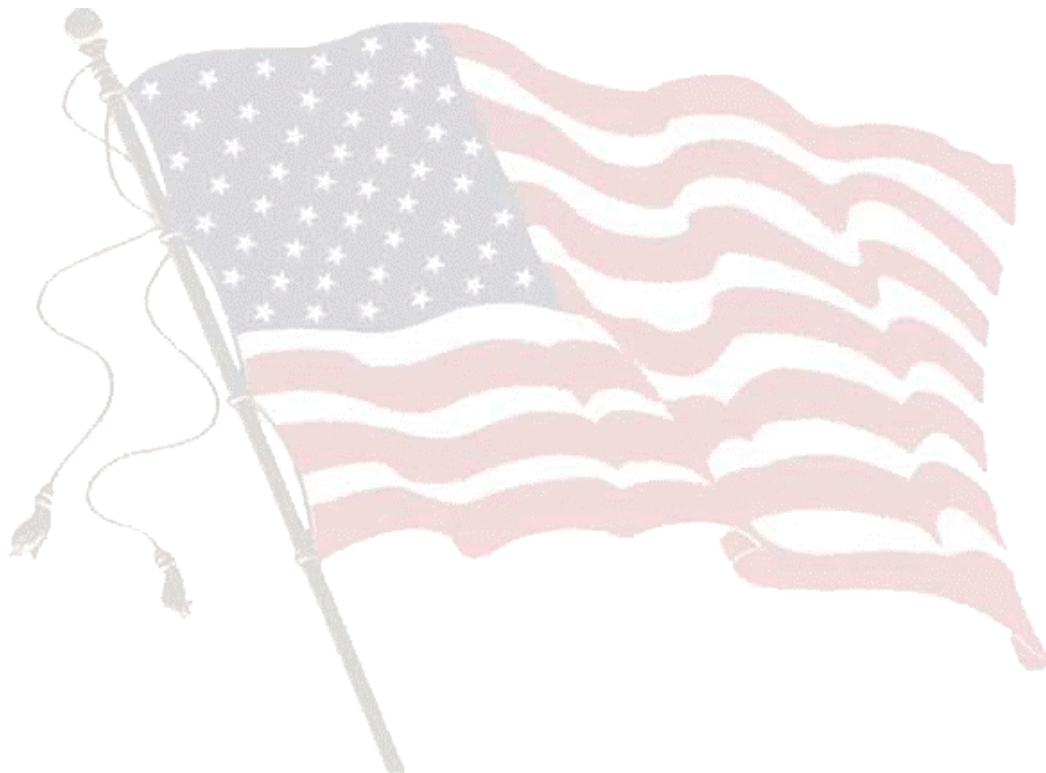
SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS (TYPE OR PRINT)	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to (1) certify that you have access to the information indicated above or (2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

***NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.**



Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration
under contract DE-AC04-94AL85000.

